The Cyber Threat to Nuclear Stability

February 12, 2016

By Paul Bracken

Paul Bracken is Professor of Management and Political Science at Yale University. He is author of *The Command and Control of Nuclear Forces* (Yale University Press, 1983); *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (HarperCollins, 1999); and *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (Times Books, 2012). He is currently working on a book on stability in the second nuclear age. He is a member of FPRI's Board of Advisors.

Abstract: *The thesis of this article is that cyber war technologies are spilling over into precision strike and nuclear mission areas. The result will transform deterrence and arms race stability and lead to other significant changes. The driver behind this is a combination of long standing problems with mobile missiles along with new technologies not usually factored into strategic assessments: big data analytics, computer vision, and related information systems. When combined with drones and precision strike, the hunt for mobile missiles is becoming faster, cheaper, and better. The implications of this finding vary by country, but will shape major power nuclear modernization, crisis stability among secondary powers, and conventional attack of nuclear deterrents.*

Air Force Staff and civilian personnel concentrate on exercise scenarios during "Cyber Guard 2015" in Suffolk, Va (DoD photo by Marvin Lynchard.)

The rising alarm to date over cyber security has focused on pilfered files, disruption of electricity and communications, and hacks of commercial and military computers. But a more serious form of cyber threat is now apparent. Cyber attacks can destabilize nuclear deterrence because they are a key element in locating mobile missiles, which became the foundation of deterrence among the new nuclear states in the Middle East, South Asia, and East Asia, thereby upsetting the embryonic nuclear stability that appears to have developed in these regions. The driver for this is not the hacking of command and control (e.g., loading malware into the firing circuit of a nuclear missile so it is unable to launch). Rather, it arises from the integration of cyber weapons and other technologies—especially drones, precision strike, and data analytics. Such an integrated system provides a remarkable ability to hunt mobile missiles that are the deterrent backbone of the new nuclear powers. Mobile systems can be found, their movements tracked, and then destroyed, using conventional or nuclear strikes. The technologies for doing so have received enormous impetus in recent years from both business and military interests.

A remarkable, decades-long interaction between strategic postures is playing out before our eyes. In the 1990s, North Korea, Pakistan, India, and Israel began to base their nuclear deterrents on mobile systems. Even some non-nuclear (so far) states (e.g., Saudi Arabia, Syria, Iran), also shifted to mobile missiles. The impetus for this shift was the United States' decisive success with precision strikes in the first Gulf War, Kosovo, Iraq, and Afghanistan. Since almost any fixed target is vulnerable, the militaries of many states believed that mobile systems were able to offer a way out to avoid destruction by a precision conventional attack. But this situation is now changing because mobile systems are not nearly as survivable as was believed a decade ago. Long recognized weaknesses in mobile systems have combined with new, cutting edge search technologies to strip features that seemed to assure survivability. This development has considerable strategic implications. For one thing, it enhances the possibility of a surprise attack by a smaller, new nuclear power against another.

In addition, nuclear modernization by major powers, like the United States, Russia and China, will take place in a *cyber* environment, where the *search* for mobile systems will be cheaper, faster, and better. This is a radically different information environment than the one that characterized the Cold War or the era of the "revolution in military affairs" (RMA) of the late twentieth century. Then, only *accuracy* was improving while s*earch* continued to be slow, costly, and spotty. How the United States, China, and Russia build cyber into their modernization programs will be a contentious issue. The way they deal with secondary nuclear states (e.g., tracking their deterrents, information transfer to regional allies and the like) will also be important. Extended deterrence, for example, will require new information structures that balance regional deterrence with stability.

Strategic Postures

A strategic framework rather than a predictive academic theory is the first requirement for any coherent discussion about nuclear weapons. Without it a debate about strategy and modernization, biases and politics lacking the rational context that

serious policy research demands will dominate. Any real problem—modernizing the U.S. nuclear posture, countering China, dealing with North Korea—will be so complex that predictive academic theories are unlikely to be of much use. While a good strategy requires such a framework, it must be tempered by details that are specific to context, country, and time frame.

One such framework was developed in the Cold War and offers insights into the dynamics of a second nuclear age. This nearly forgotten framework was called "max-min," and it defined a strategic posture in terms of two factors: *accuracy* and *search*.[1] *Accuracy* describes how close to its target a system can deliver a warhead. Accuracy is measured in terms of "circular probable error" (CEP), defined as the radius of a circle, centered on the target, within which 50 percent of the warheads are expected to land. A smaller CEP indicates greater accuracy. While the Cold War framework focused on nuclear warheads, the concept applies to conventional precision weapons as well, since they are also capable of destroying non-hardened nuclear targets.

Search is defined as the time it takes to fix a target's location, measured in hours or days. A surrogate measure of search is the amount of money put into programs and technology. For example, the dollars invested in the U-2 reconnaissance program, anti-submarine warfare (ASW) assets and spy satellites were also measures of search.

Analysts have understood the significance of breakthroughs in accuracy for some time.[2] These are the backbone of the precision strike revolution. What is not appreciated yet is that a revolution in search technology in recent years promises to have an equally large impact.

The term "max-min" arises from the idea that in a first strike nuclear attack, the attacker attempts to *minimize* retaliation while the second striker attempts to *maximize* the retaliatory blow. When the theory was first developed in the mid-1960s, U.S. policymakers assumed that the Soviet Union would strike first and that the United States would retaliate.

It is important to understand that the two strikes occur sequentially. The order of moves matters. If it changes (e.g., the United States strikes first), so do the results. Therefore, max-min ≠ min-max, as in the mini-max theorem of game theory. Thus, this *is not* game theory. There is no definition of game theory's mixed strategies, so bluffing analogies with poker—central to game theory analyses of

[1] Max-min theory came from operations research. See John Danskin, *The Theory of Max-Min, and Its Application to Weapons Allocation Problems* (Berlin: Springer-Verlag, 1967); and T.E. Phipps, Jr., *Optimum Systems Choice for Strategic Retaliation: An Application of Max-Min Theory*, Report 67-59, U.S. Naval Ordinance Laboratory, White Oak, MD, April 1967.

[2] See Thomas G. Mahnken, "Weapons: The Growth and Spread of the Precision-Strike Regime," *Daedalus,* Summer 2011, pp. 45-57; and Mike Aaronson, Wali Aslam, Tom Dyson, and Regina Rauxloh, eds., *Precision Strike Warfare and International Intervention* (New York: Routledge, 2015).

nuclear strategy—do not exist here.[3] Max-min deals with long-term competition rather than short-run moves. The time frame of the max-min analysis is thus closer to net assessment.[4] The focus is on multi-year efforts to build a strategic posture after analyzing what one's opponent has chosen. The "moves" are investments in intelligence systems such as ASW, satellites, and other search technologies; and weapons, such as fixed and mobile missiles, bombers, and submarines. Because all of this includes the information processing architecture, as well as nuclear weapons, a better name is "strategic posture." The term "nuclear posture" is reserved for the weapons alone.

Max-min theory posits that different types of weapons have different kinds of vulnerabilities. Some weapons are easy to find, but hard to destroy while others are hard to find, but easy to destroy. Consider fixed site inter-continental ballistic missiles (ICBMs). After both sides had invested in spy satellites and other national technical means, during the 1950s and '60s, U.S. missile sites proved comparatively easy to find. Soviet analysts could get a good fix on U.S. ICBM locations by examining Congressional testimony, spies, media reports, and intercepted messages. The same held true of Soviet ICBMs, as well. Indeed, the search for them was a major driver of U.S. reconnaissance programs.

ICBMs were easy to find, but they were hard to destroy. There were several reasons for this. First, missile silos were separated enough that an attacker's single warhead could not destroy more than one silo. In addition, they were hardened to minimize the ground shock from a nuclear explosion. An attacker had to land multiple warheads very close to a silo to destroy it with any degree of confidence.

On the other hand, ballistic missile submarines were soft targets. A single nuclear or conventional weapon, such as a torpedo or cruise missile could easily destroy a submarine at firing depth—if it could be reliably located. The search for fleet ballistic missile submarines (SSBNs) drove enormous U.S. expenditures. But the mathematics of search was against the searcher. Technologies such as sonar, ocean surveillance and radar were not reliable enough to locate most enemy submarines. It was possible to locate a submarine by luck, but luck was not enough to inspire confidence in an attack on SSBN fleets.

Of course, it was also possible to destroy SSBNs by means of an area attack: launching a barrage of nuclear warheads against an expanse of ocean with the goal of destroying any submarines in the barrage zone. Certainly, the vast expenditure of nuclear ammunition required would quickly exhaust even the large arsenals of the Cold War.

Bombers fit into the max-min framework, too. Parked on known airfields, nuclear armed aircraft were easy to locate and destroy. But if they deployed to alternate airfields—and there were enough of these fields—then the bombers were hard to find, too. During the Cuban missile crisis of 1962, Strategic Air Command (SAC) dispersed its bombers to alternate fields, including commercial airports in

[3] See, for example, Thomas C. Schelling, *The Strategy of Conflict* (New York: Oxford University Press, 1963).
[4] See Paul Bracken, "Net Assessment: A Practical Guide," *Parameters*, Spring 2006, pp. 90-100.

Boston, Detroit, St. Louis, and other cities.[5] This was the only time during the Cold War that SAC executed a full-scale dispersal of its bomber force.

Airborne alert could also reduce bomber vulnerability by placing bombers in airborne holding positions so that they could not be located. SAC greatly intensified its airborne alert during the Cuban missile crisis. But, of course, the major problem with both dispersal and airborne alert is that it was extremely expensive to maintain over any extended period of time, and it places enormous stress on the air crews. Even with SAC's substantial budget, and its highly professional crews it was hard to keep an alert posture for any length of time. It was also dangerous. Several B-52s crashed while carrying nuclear weapons. The rarity of SAC bomber dispersals and alerts illustrates the practical problems associated with operating mobile systems.

Table 1 summarizes the types of Cold War vulnerabilities in terms of max-min theory. The goal was to hedge against a homogeneous type of vulnerability because technology breakthroughs might jeopardize national survival. Thus, stable nuclear deterrence required a mix of different types of vulnerability. This was the rationale for the nuclear "triad."

Table 1: Types of Cold War Vulnerabilities

Easy to Find, Hard to Kill	**Hard to Find, Easy to Kill**
Silo-based ICBMs	SLBMs
	Dispersed bombers or airborne alert

The Shift to Mobile Missiles

The shift to mobile delivery systems for both conventional and nuclear weapons began in the late twentieth century. Russia, North Korea, China, India, Pakistan, Iran, Iraq, Israel, Saudi Arabia, Egypt—and many others—took this path.[6] Although we have a great deal of detailed information about these weapons, including range, payload, accuracy, and type of transporter, it is of limited utility. Indeed, it often leads to intellectual and organizational chaos. Collecting ever more detail misses the big picture, which is the fact that a multi-decade interaction between strategic postures—mobile delivery systems on the one hand and precision strike improvements on the other—is currently underway.

The shift to mobile missiles is a response from the growing accuracy of precision strike weapons. Fixed missile and aircraft sites are vulnerable. The exact mix of mobile and fixed missiles varies from one country to the next depending on context. The obvious choice to counter such accuracy is a mobile missile system that is difficult to locate with any degree of confidence. *This is why it is so significant that mobile systems are becoming vulnerable*. Many countries have made enormous investments

[5] "50 years ago, Tampa was on front line of Cuban Missile Crisis," *Tampa Bay Tribune*, Oct. 13, 2012.

[6] For an overview, see Randy Huiss, "Proliferation of Precision Strike: Issues for Congress," Report R42539 (Washington, D.C.: Congressional Research Service, May 14, 2012).

in them and have even bet their national survival on them. An increase in their vulnerability, then, has immense consequences for deterrence and arms race stability. Countries that believed they were buying deterrence will soon learn that this is not the case. And arms races that looked stable in a classic deterrence framework are likely to look much less so.

The Vulnerability of Mobile Systems

Two factors affect the vulnerability of mobile systems. This is important to understand because the argument here is not that a pure technology breakthrough has made mobile systems vulnerable. The two factors complement each other.

First, mobile systems (missiles and bombers) have inherent problems that were recognized during the Cold War.[7] These problems were substantial enough to dissuade the United States from deploying land-based mobile missiles as part of the strategic triad.

While the United States did, in fact, deploy theater level intermediate range mobile systems, primarily the nuclear Pershing 2 in Europe, the problems limited the number of these systems.

The *second* factor is that cyber technology—not only computer viruses, but also the new technologies of cell phone, package, and vehicle tracking, as well as technologies for distributed car services such as Uber, Lyft, mobile social nets, customer tracking in retail stores, fleet management, distributed sensors on drones and highway cameras, and automated license plate readers—has revolutionized the business of *search* in a way that precisely exploits these weaknesses.

Another important technology is the ability to analyze large amounts of data and integrate them into a form to make better targeting decisions.[8] The integration of data from cell phone tracking with drone video of cars and trucks, pings of mobile computers with nearby cell towers, phone cameras and radio-frequency identification (RFID) tags, have developed to a high art form. They are widely used in business today. Pattern recognition, system visualization, and predictive analytics are not a futuristic possibility, but the backbone of operations at Walmart, Amazon, Federal Express, Uber, and in many other industries. Thousands of companies now sell this technology. Business schools teach it. There is a large and growing body of expertise in the world, in all major countries, that install it.

As noted earlier, mobile missiles have suffered from significant problems since their origin. Table 2 lists the problems for mobile systems, which make it easier to understand how the hunt for mobile missiles is undergoing a remarkable transformation.

[7] See Herman Kahn, *On Thermonuclear War* (Princeton University Press, 1960), pp. 265-269.
[8] For an overview of this technology, see Patrick Laube, *Computational Movement Analysis* (Heidelberg: Springer Briefs in Computer Science, 2014).

Table 2: Problems Associated with Mobile Systems

• Mobility Defined
• Geographic Restrictions on Mobile Systems (land, sea, air)
• Hacks of Mobile Command and Control
• Outsized Alert Signature
• Soft Targets
• Area (Barrage) Attack
• High Operating Costs and Demands on Crew
• Operational Security (information leaks, "tells")
• Peacetime and Pre-Conflict Attack

Problems of Mobile Systems

The first problem with mobile missiles is that "mobility" is rarely defined. The long-range mobile missiles of North Korea, India, Pakistan, and other countries are not so much mobile as they are portable. Even this is being generous. These missiles can be moved only with significant effort and time. The belief that mobile missiles can be transported off road and on, and can be made operational in a short time, is an illusion. The idea that a missile transporter, erector, launcher (TEL) driving at 45 m.p.h. around North Korea, Pakistan, Iran, or Israel, ducking under the cover of overpasses, quickly setting up—and then breaking down and moving rapidly to another site—ignores just how many interacting parts these systems have.

Mobile missiles require support crews and equipment: fuel trucks, electronic and vehicle technicians, a warhead crew, lift operators and field support of these operators as well. Moving a missile without its support crew is impossible. If a critical piece of gear fails (e.g., the pneumatic system that erects the missile into its firing position), the missile remains non-operational until the support equipment is repaired. Some problems may be fixed by the organic repair crew. Other problems require support from higher headquarters.

All of this means a great deal of communications and travel. Communications can be tracked. Drones can video the moves. A fuel truck or communications van, rather than the missile carrier itself, may be the clue to a mobile missile's location. Moreover, in today's world, the likelihood that all the crew members will turn off their cell phones is improbable. Informal, unofficial communications are likely to be an especially significant factor in revealing the location of a mobile missile.

Tracking moving targets, such as trucks and people, is the purpose of the new search technologies. One of Edward Snowden's revelations is that the United States reportedly has developed a technology called "Sting Ray" that tricks cell phone networks into capturing calls, phone location, and caller and called identities. It delivers this information to police and other authorities. Sting Ray is now widely used in law enforcement and intelligence. Commercial software is available for it.[9] When combined with automatic license plate tracking, it gives reliable data about persons of interest.

Geographic constraints on mobile missiles are another problem. This means, obviously, that support units will cluster around particular roads, airfields and ports, which narrows the search area, enabling intelligence assets to focus on just these zones. A country can rehearse its attack against the practice exercises of its enemy for years to see where its missiles move, how long it takes to set up and break down, and how long they remain in one spot. They can analyze the communications associated with each of these actions.

Command and control of a mobile nuclear force requires much more communications than for a fixed one. All of this must be done by a radio transmission, whether analog or digital, over a military circuit or cell phone, or via a satellite. It cannot be done over fixed lines, as with stationary missiles. It also has to be practiced. Trying to do it the first time is likely to create lucrative targets from the backed up vehicles, requests for new orders, and desperate transmissions in the clear over insecure channels. *This is also a golden opportunity for cyber attacks.* Deceptive orders ("do not fire") modeled on hacked real ones, jamming of key circuits, and requests to "identify your current location" can be created in advance and gamed out against the observed data of practiced exercises.

False orders can be injected into mobile missile command systems in peacetime just to see how they react. Repeatedly probing the enemy command and control system with innocuous messages can create a good picture of how it operates.

Mobile missiles produce an outsized alert signature. Their alert rate, movement, and readiness are cut back to safe, acceptable levels most of the time for this very reason. When an alert occurs there is a visible surge of movement, message traffic, transmission of code words, and requests for clarification. Nuclear warheads are moved from bunkers closer to their missiles. Special guard units and technicians have to be readied. All of this is highly visible.

The shock of seeing an actual, rather than a practice, alert could lead to psychological overreaction. This is another problem. For this reason it may be delayed, as a kind of political signal. But delaying an alert may create a golden opportunity for a disarming strike on the unprepared missile force. This may be especially risky if the attacker believes it can get away with only conventional attacks. A conventional attack may work or it may not. This could create a situation where conventional strikes on the nuclear deterrent have failed to destroy it, and the potential for nuclear escalation is increased greatly. The attacked party may well

[9] "Fake Cell Phone Towers Allow the Police and NSA to Keep Track of You," *Newsweek*, Sept. 5, 2014.

believe that the nuclear follow on is coming soon, and that it must strike first before its systems are destroyed.

A nuclear strike is much more likely to do what a conventional attack could not. This is because mobile missiles are soft targets. Most mobile missiles have either no protection at all, or are contained in a thin skin tube built for lightness and portability—not survival. A nuclear weapon, even a fission weapon of the kind deployed by the new nuclear states, can easily generate 1000 psi of overpressure. (A severe category 1 hurricane with winds of 200 mph generates only a .8 psi overpressure.) Even a miss can knock over a missile truck and its support vehicles. Precision strikes with cluster or pointed steel projectile (flechette) warheads designed to destroy airplanes on the ground are likely to be devastating against mobile missiles. Conventional weapons may also be used in barrage attacks if the shooter is not certain of the exact location of the target. Area attacks do not require pinpoint location.

The high costs of operating a mobile force means that in many countries training will not be taken as seriously as it needs to be. In peacetime, it will be seen as expensive. Operations may get sloppy. In a crisis, provocative moves may be seen as dangerous. For this reason, the variance of performance is likely to be considerable across countries, and within them. Different crews will perform differently.

A related vulnerability is operational security (OPSEC), which although a problem for all military operations, is especially so for mobile systems because survival, and deterrence, depend on keeping their location secret. Every drone pass may be suspected of tipping off the enemy.[10] Tips might come from a cell phone call, an individual seeking photos with a camera phone, or tagging with RFID chips. Any of these tips can give away the location to enemy intelligence, or cue a drone for a closer look.

Even if extraordinary secrecy is imposed on missile movements, there are "tells" that undermine operational security. A "tell" is a term from poker to describe a change in a player's behavior that provides clues to what kind of hand he has. Cyber intelligence collects all kinds of information that traditional military radars and satellites do not. There is no guarantee that these tells are indicative of actual behavior or intention, of course. The psychology in these situations gets extremely complex.[11] It is going to be even more so with new technologies that search cell phone nets, roads, and airfields.

Finally, insider attacks on mobile missiles are always a danger because insiders know the weaknesses. During the Cold War, large arsenals were widely separated making sabotage difficult. In the case of a small power, sabotage could take out a significant part of its nuclear deterrent. It is likely that a new special force

[10] The crisis management implications of wider drone use are described in Michael J. Boyle, "The Race for Drones," *Orbis,* Winter 2015. Boyle discusses the use of drones for signaling and testing the will of an enemy.

[11] Robert Jervis, "Deterrence and Perception," *International Security*, Winter 1982-83, pp. 3-30.

of spies and saboteurs will be stood up by many countries for this very purpose. Such units might be pre-deployed, or run as sleeper cells to report on mobile missile locations in a security emergency.

Big Data Analytics

Data analytics is the linchpin technology in the hunt for mobile missiles. Like the pin passed through the end of an axle to hold a wheel in place, data analytics holds the search for missiles together so that it does not degenerate into an uncoordinated hash of drone video, phone tracks, and cyber espionage. Drones, intercepts, and hacks might locate some missiles. But what is required is an integrated program that systematically does it.

This is why data analytics is so important. It tells users how many drones are needed, how deep it needs to penetrate into a phone grid, and how often it needs to update its picture of a battle space. A higher level strategy is needed to organize limited search resources, and to integrate with one's own forces to act on the information collected.

Big data analytics is the process of analyzing large, diverse data sets (voice, text, video, images, radar, signals, telemetry) to uncover hidden patterns, unknown connections, and other insights to make better decisions. Business has used it to reengineer their core operations. Progressive Insurance, for example, uses it to micro-segment drivers—accident record, credit score, miles driven, and home neighborhood. This data is combined with driver behavior taken from tiny sensors plugged into the car. Acceleration, night driving, abrupt braking, and speed are recorded.[12] This combined data gives powerful insights into who is a good or bad driver, and hence, a risk for Progressive.

Data analytics has been developed mainly by and for business.[13] It is used by companies around the world and is disrupting retailing, health care, transportation (Uber and Lyft), hospitality (Airbnb) and package delivery in the United States, Europe, China, India, Japan, and nearly everywhere else. Data analytic packages are sold everywhere. Consulting firms offer implementation services. Business schools teach how to use it, and how to tie it in with strategy.[14]

Analytics is a key technology in business competition. These "wars" should be studied by strategic analysts and the military for their lessons learned. Wal-Mart built its success on optimized global supply chains and rapid delivery of products to stores. Then, along comes Amazon, a company that was born digital. Its 65 U.S. distribution centers are built for the e-commerce age, not the suburban sprawl world of the 1980s. Wal-Mart is fighting back, but must overcome a legacy of dozens of

[12] Robert Passikiff, "Progressive Adds 'Bad Driver' Surveillance to Snapshot Telematics," *Forbes,* March 31, 2015

[13] For an overview of this field, see Nathaniel Lin, *Applied Business Analytics, Integrating Business Process, Big Data, and Advanced Analytics* (Pearson FT Press, 2014); and Sudi Sinha, *Making Big Data Work for Your Business* (Pakt Publishing, 2014).

[14] A recent web search turned up over 100 MOOC courses on big data analytics, mostly offered by leading business and engineering schools. Nearly all of them were free.

different software platforms.[15] One insight Wal-Mart has learned is that customers respond differently to products when online compared to being physically present in a store. The whole basis of Wal-Mart's "cut, cut, cut" pricing worked in stores, but online the incentive is more to upsell and link related products to micro-segmented customer tastes.

Pizza wars between Domino's and Pizza Hut also use analytics as a key weapon.[16] These firms "slice" customers into 6,000 distinct groups, based on tastes, purchase channel (mobile phone, web, pickup, delivery), and income. The pizza business is changing from a food to a delivery business, so wait times, congestion, and routing become ever more important.

One might think that these examples do not apply in international affairs because they involve cooperative agents. But this is not the case. Volkswagen did not view regulators, or for that matter customers, as cooperative agents when they recently deceived environmental regulators. They used data analytics to sell diesel cars in different countries, and used it to reprogram the software controlling automobile pollution to deceive regulators.

There are many lessons from these cases for the military. For one, experience suggests that it is the integration of different types of information that yields the biggest payoff. Consider a hypothetical example. Suppose a country collects video of enemy mobile missiles from drones and cell phone cameras taken by its informants. This happens in peacetime over many years. Suppose, further, that it has hacked into security camera networks of local police and around government buildings. Some cameras will show license plates, and these numbers can be fed into an automatic license plate reader working with a hot sheet of people in the chain of command.[17] Such tracking could locate wartime headquarters or alternate command centers.

Next, movements of the missile transporter and support vehicles and the nuclear warhead crews are pulled together and analyzed along with this data. Each operation is broken down into segmented parts: the fueling of the vehicles; the time it takes to brace the missile truck; how long it takes to elevate the rocket; the distance between warhead and the missile is recorded; the type of cover the missile usually seeks, for example, near hillsides, overpasses, or in forests, is noted.

There are hundreds of parameters, and enormous amounts of data on video. There could be scores of missiles exercises or partial exercises over the years. Some of these might only involve raising the missile to see if the lifting mechanism worked. Others might include support vehicles. A field called computer vision has been

[15] Kim S. Nash, "Wal-Mart Revamps E-Commerce Technology as Amazon Applies Pressure," *Wall Street Journal,* Nov. 25, 2015.

[16] See Larry Dignan, "Pizza Hut eyes digital, data transformation in pizza wars," ZDNet, June 26, 2015.

[17] A hacked security camera system can be partially controlled, to tilt and pan cameras in certain directions. For an overview of state-of-the-art analytics in camera networks, see Amit K. Roy-Chowdhury and Bi Song, *Camera Networks, The Acquisition and Analysis of Videos Over Wide Areas* (Morgan & Claypool, 2012).

developed to automate the analysis of this information.[18] It has been used to monitor shoppers at store checkout lines from the enormous amount of security footage that exists to prevent shoplifting. There is far too much of this data generated by big box retailers to ever watch it manually. So an automated process was created. Basically, the footage is digitized and fed into a computer. The output is the statistical distribution of time it takes to pull out a credit card, how many items are purchased, the mix of items, and whether a customer chats with the checkout person. Computer vision automates the analysis. Applying this technology to reading drone and cell phone video would provide statistical distribution data on the micro-segmented analysis of a missile's moves.

These data could then be correlated with the crew's cell phone traffic—the number of calls, caller and called identities, the military rank and position of the caller in the command chain. Social media texts and traffic over official radio circuits could be included. Communications between the missile crew and the warhead guards might be brought in. The integration of this diverse data is likely to reveal patterns that the country owning the missiles does not even know. Finally, traditional military collectors and sensors—space-based radar and moving target indicator radars, and signals intelligence—would be brought into the assessment.

This example illustrates how search is getting faster, cheaper, and better. The technologies behind it are among the hottest in business, venture capital, and in research in business and engineering schools. There is massive field experimentation taking place as companies try these approaches in actual conditions.

This last point is important. Big data analytics is of little use if it is not tied into operations. Forces have to be agile in order to use it. Certainly, Amazon, Wal-Mart, Pizza Hut, and others, collect more information about their customers. But they have used it to change fundamentally the way they operate. Big data analytics in the national security space is likely to be no different.

The Maritime Theater

In the Cold War, submarines were the gold standard of survivability. For this reason they loomed large in the superpower nuclear force mix. But that was a long time ago, in a different technological era. Many of the arguments about land-based mobile missiles and bombers also apply in the maritime theater. Indeed, the original max-min framework was to provide insights about the mix of ICBM, bomber, and submarine based deterrents, a subject that is becoming more important. The United States, China, Russia, India, Pakistan, Israel, France and Britain have nuclear weapon submarine programs. (Modernization requires that a mix of weapons be evaluated carefully.) Some countries also have nuclear weapons on surface ships.

The maritime theater presents a different search environment than land. Yet technology advances make search better, faster, and cheaper, compared to a decade ago. Drones can search wide areas. Espionage such as port watching, tagging enemy

[18] See Giovanni Maria Farinella, Sebastiano Battiato, and Roberto Cipolla, eds., *Advanced Topics in Computer Vision* (Springer, 2013).

ships with geo-location sensors, and cyber attack of long haul communications and platform IT are all threats to seaborne nuclear forces.

While there are many particular national cases we could examine, of special interest is the one between China and the United States. The nature of the Asia Pacific theater is especially conducive for a framework organized around accuracy and search. U.S. maritime power depends on fixed bases (e.g., Guam, Kadena, and others that are "easy to find and easy to kill"), and on ships and submarines that are "hard to find but easy to kill" if they were found. The Pacific theater thus, has many instances where *search* is critical. Drones, satellites (and anti-satellite weapons), signals intelligence, spies and ASW are in one way all about search.

In addition, China's growing search capabilities are a distinctive feature of this long-term rivalry. The close monitoring of U.S. forces is reflected in tight hugging, drone and satellite passes, and information warfare probes of U.S. forces and support ships. This vast effort needs to be organized by some method such as data analytics. And this system needs to be linked to targeting of its mobile, cruise, and hypersonic missiles.

China is choosing its strategic posture based on a careful study of U.S. vulnerabilities. It fits the framework of a first striker trying to minimize the residual capability of U.S. forces. The United States, in turn, is trying to maximize its own survivability, with an emphasis on concealment, disruption of China's search ability, and speed. The United States is not trying to deal with the threat purely by increasing force structure. Most of the proposals to counter China's sea denial amounts less to deploying more missiles than to disrupting the information flows supporting China's search effort.[19]

In the late 1990s, the rivalry in the western Pacific was still dominated by *accuracy* rather than *search*. China could target U.S. bases and assign missiles accordingly. But China could not fix the location of U.S. ships. This uncertainty had important effects on taming any instinct to use force. What is new is that China's investments in search have begun to pay off.

Strategic Implications

The thesis of this article is that *cyber is spilling over into precision strike and nuclear*. Cyber technology increases the performance of systems in these other areas. It improves precision strike, which makes it effective against a wider class of targets. When these targets are nuclear weapons, it offers a way to take out these forces, either with conventional or nuclear attack.

Treating these three technology areas individually, without their interactions, must give way to a broader integrated assessment. Absent a holistic framework, investments and innovation will be skewed badly. At a minimum, it helps to replace the tendency of experts to frame problems within their own "stovepipe." Thus,

[19] See Jan van Tol, et al., "AirSea Battle: A Point-of-Departure Operational Concept," Center for Strategic and Budgetary Assessments, May 18, 2010.

cyber defenses counter cyber attacks. Nuclear weapons deter nuclear attacks. This un-integrated analysis overlooks how cyber improves precision strike, and how this makes conventional first strikes against mobile nuclear weapons achievable.

Among major powers, the United States, Russia, China, India, Britain, and France, the danger of any of them attacking each other's nuclear forces seems low at present. Yet, they have ignored the U.S. call for a "world without nuclear weapons" and instead have undertaken nuclear modernization. The United States has lagged here. But the terms of the debate have changed in the last few years. The United States is set to modernize its nuclear force, although the exact form is as yet inconclusive.

And for the purposes of this article, this is precisely the point. U.S. nuclear modernization is unlikely to be a business as usual rehash of its Cold War posture because it will take place in a very different technological era. A modernized U.S. nuclear force must consider the strategic postures of other countries. Here it seems hard to believe that others will not exploit the broadened capability that cyber technologies offer. It is pointless to design a U.S. force for a bipolar world that no longer exists.

Others are already modernizing for the world of the twenty-first century. China's sea denial strategy in the western Pacific integrates cyber with precision strike. This creates a *de facto* escalation framework of Chinese nuclear deterrence of U.S. conventional strikes. It makes little sense for the United States to pretend that this has not taken place. The U.S. effort to remove nuclear weapons from international affairs is in a certain way quite laudable. But the failure to eliminate nuclear weapons altogether must be acknowledged. Other countries, China and Russia, in particular, have made strategic choices that take a more holistic approach to the technologies analyzed here. Even if the United States were to separate cyber, precision strike, and nuclear, there is little reason to believe other countries would follow suit.

Another implication of this analysis is that countries with high tech innovation capacity will have an edge in whatever posture they choose. Silicon Valley matters. It matters because it created the cyber revolution in the first place, and it will matter in the future as other major powers try to copy it or reproduce it in their own way. There are likely to be high levels of R&D in all of the major powers for this reason. Some will do better than others. And there is a risk that the United States may become complacent about its leading position. But falling behind on this front invites trouble.

High tech defense innovation may be like table stakes, something that a country needs simply to ensure that it stays a major power. Or it may resemble earlier times, when innovations brought temporary advantage, only to be offset by other innovations after a few years. There are many different patterns possible. U.S. leaders must be aware of where technology is heading since falling behind may invite other countries to exploit the vulnerabilities created by this.

A further implication for the major powers is the importance of not relying on a homogeneous nuclear deterrent. There were good reasons for the U.S. nuclear triad, and uncertainties about world order are greater today than in the Cold War. The overlay of cyber technology on to the international system makes this even more

so. What this suggests is that we need very good reasons to eliminate one of the triad's legs (e.g., ICBMs or bombers). The arguments made for this, as yet, have been unconvincing. The cost-benefit studies of maintaining nuclear deterrence without ICBMs are highly suspect since they discount technological surprise in an era during which technology has disrupted one industry after another.

Turning to the strategic implications of cyber for stability among secondary powers, the situation is alarming. When striking first has a large advantage it creates a surprise attack problem. For this reason, nuclear deterrence in East Asia, South Asia, and the Middle East is likely to be more tenuous than anyone has thought. Deterrence in this region is not a mere replay of the Cold War.

When secondary nuclear states also face a significant threat from a major power this is all the more the case. North Korea and Pakistan stand out here. They face regional enemies who are quite capable of deploying cyber and precision strike threats against their deterrents. North Korea must deal with South Korea and the United States. In addition, Pyongyang is unlikely to dismiss China as a threat when it comes to tracking its mobile missiles. Pakistan faces India, a country now making a concerted push in the direction of cyber attack and precision strike. Information technology is one of India's strategic industries. Perhaps it has not figured large historically in India's military posture. But no thinking person who studies this can doubt that the situation has changed fundamentally since the Mumbai attacks of 2008. Pakistan is also unlikely to dismiss the United States as a threat when it comes to tracking the location of its mobile missiles and navy.

There are obvious ways to counter the threats to small nuclear forces (small defined here relative to the nuclear forces of the major powers). One counter is to acquire more weapons, which makes it unlikely that an entire force can be taken out with a first strike. This appears to be the case with many small nuclear states. While North Korea possessed only a handful of nuclear weapons a few years ago, today some analysts believe that Pyongyang will be able to field a force of 60-80 warheads in the 2020s. Pakistan also is building up its nuclear forces rapidly. This shows the strategic interactions between postures discussed here.

How major powers interact with the secondary powers will be increasingly important. The United States, for example, should make it clear that any general alert of North Korea's mobile nuclear forces is unacceptable and destabilizing. It is a good thing for Pyongyang's leaders to understand that such moves may draw fire. This is an overlooked issue in much of the literature. There is a difference between deterrence of nuclear attack, and deterrence of a nuclear provocation—like putting mobile missiles on alert.

In the seven decades that nuclear weapons have existed, there have been other threats to stability from technology. Improved ICBM accuracy, multiple independently targetable reentry vehicles, and missile defense have changed the strategic balance in the past. We again face this prospect, now from cyber technologies. What is different this time, and troublesome, is the larger number of decision-making centers whose collective actions are shaping the international order. This creates questions of political and moral responsibility for the major powers, of

how to enforce order on a system that may simply have too many states armed with nuclear weapons in it. This is one of the great questions of our era, and one that needs sober debate.